(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 December 2004 (23.12.2004)

PCT

(10) International Publication Number
WO 2004/111752 A3

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number:
PCT/NL2004/000422

(22) International Filing Date: 14 June 2004 (14.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PCT/NL03/00436 13 June 2003 (13.06.2003) NL

(71) Applicant *(for all designated States except US)*: **ORBID LIMITED** [IE/IE]; Wil House, c/o Oonagh Hayes, Shannon Business Park, Co Clare Shannon (IE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **TEL, Teunis** [NL/NL]; 13 Esserlaan, NL-9722 SK Groningen (NL). **WARD, Scott, MacDonald** [US/NL]; 31 Zuidlaan, NL-2111 GB Aerdenhout (NL).

(74) Agent: **MERTENS, H., V.**; Exter Polak & Charlouis B.V., P.O. Box 3241, NL-2280 GE Rijswijk (NL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

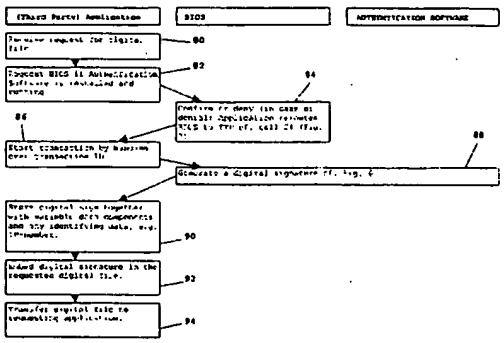
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
17 March 2005

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR PERFORMING A TRANSACTION AND FOR PERFORMING A VERIFICATION OF LEGITIMATE ACCESS TO, OR USE OF DIGITAL DATA



(57) Abstract: A method for performing an electronic transaction is disclosed. The method provides authentication data and authentication software to an electronic device and preferably stored in a secure storage location or other location inaccessible to the user or the operating system of the device. When digital data is requested from a transaction party that requests a digital signature, the authentication software is activated to generate said digital signature from the authentication data. Next, the digital signature is provided to the other transaction party, which then provides the requested digital data. The digital signature may be embedded in the requested and provided digital data. Further, a method for performing a verification of legitimate use of digital data is disclosed. Digital data digitally signed according to the present invention may only be accessed if the embedded digital signature is identical to a regenerated digital signature that is regenerated by the authentication software, using user inaccessible authentication data installed on the device. If the embedded and regenerated digital signatures are not identical, the data may not be accessed and an error signal is generated.

WO 2004/111752 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Intern...l Application No
PCT/NL2004/000422

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/112162 A1 (COCOTIS THOMAS ANDREW ET AL) 15 August 2002 (2002-08-15) abstract paragraph [0095] paragraph [0043] paragraph [0067] -----	1-27,29, 30
X	US 2002/112171 A1 (GINTER KARL L ET AL) 15 August 2002 (2002-08-15) abstract paragraph [0602] paragraph [1302] paragraph [1085] paragraph [1813] paragraph [1913] figures 6-8,35-38,68-71,75 ----- -/--	1-27,29, 30

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 October 2004	25/01/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kleiber, M

Form PCT/ISA/210 (second sheet) (January 2004)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2 338 381 A (BARCLAYS BANK PLC) 15 December 1999 (1999-12-15) abstract figures 1,5,11 page 2, line 18 - page 4, line 7 page 5, line 10 - line 22 page 6, line 11 - line 15 page 10, line 1 - line 20 page 11, line 3 - page 12, line 8 page 14, line 1 - line 18 page 17, line 5 - page 18, line 22 ---	1-27,29, 30
A	BENNET YEE: "Using Secure Coprocessors" THESIS SUBMITTED TO THE SCHOOL OF COMPUTER SCIENCE FOR THE DEGREE OF DOCTOR OF PHILOSOPHY, XX, XX, May 1994 (1994-05), page COMPLETE, XP002120312 the whole document ---	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NL2004/000422

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-27, 29, 30

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-27,29-30

   Method for perfoming an electronic transaction using authentication software.

   ---

2. claims: 28,31

   Method for encrypting digital data using a session specific key

   ---

INTERNATIONAL SEARCH REPORT

Interr I Application No
PCT/NL2004/000422

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002112162 A1	15-08-2002	NONE	
US 2002112171 A1	15-08-2002	US 6237786 B1	29-05-2001
		US 5915019 A	22-06-1999
		AU 711733 B2	21-10-1999
		AU 6326696 A	18-09-1996
		CA 2212574 A1	06-09-1996
		CN 1183841 A	03-06-1998
		EP 1431864 A2	23-06-2004
		EP 0861461 A2	02-09-1998
		JP 10512074 T	17-11-1998
		JP 2004265358 A	24-09-2004
		JP 2004005558 A	08-01-2004
		JP 2004005601 A	08-01-2004
		JP 2004139550 A	13-05-2004
		JP 2004030600 A	29-01-2004
		JP 2004005614 A	08-01-2004
		JP 2004005625 A	08-01-2004
		JP 2004005629 A	08-01-2004
		US 2003191719 A1	09-10-2003
		WO 9627155 A2	06-09-1996
		US 2003088784 A1	08-05-2003
		US 2003105721 A1	05-06-2003
		US 6253193 B1	26-06-2001
		US 6185683 B1	06-02-2001
		US 6363488 B1	26-03-2002
		US 6389402 B1	14-05-2002
		US 6427140 B1	30-07-2002
		US 6658568 B1	02-12-2003
		US 2004133793 A1	08-07-2004
		US 2004103305 A1	27-05-2004
		US 2004123129 A1	24-06-2004
		US 5910987 A	08-06-1999
		US 5949876 A	07-09-1999
		US 5917912 A	29-06-1999
		US 2001042043 A1	15-11-2001
		US 2004054630 A1	18-03-2004
		US 5982891 A	09-11-1999
GB 2338381 A	15-12-1999	AU 9175798 A	30-12-1999
		CA 2299294 A1	16-12-1999
		CN 1266520 T	13-09-2000
		DE 29824106 U1	13-07-2000
		WO 9964995 A1	16-12-1999
		JP 2002517869 T	18-06-2002